

Homework 1

Due Wednesday, April 10, at noon

Homework is due at noon on the following Wednesday. You are encouraged to work together with others, but you must write up the solutions on your own.

All numbered exercises are from Dummit and Foote, third edition.

1. (5pt) 13.1.5
2. (5pt) 13.1.8
3. (5pt) 13.2.3
4. (5pt) 13.2.13
5. (5pt) Let $m, n \geq 1$ be positive integers such that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is an extension of finite fields. Show that $m \mid n$. (Here $\mathbb{F}_{p^k}$ represents a field with p^k elements.)

HOMEWORK 1

SOLUTIONS

Problem 1 [13.1.5] Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[X]$. Prove that $\alpha \in \mathbb{Z}$.

Proof. By the rational root theorem (Prop. 11, Ch.9) if $\alpha = \frac{p}{q} \in \mathbb{Q}$ is a root of the monic polynomial and $(p, q) = 1$ then $q \mid 1$ and therefore $\alpha \in \mathbb{Z}$. $\square$

Problem 2 [13.1.8] Prove that $x^5 - ax - a \in \mathbb{Z}[X]$ is irreducible unless $a = 0, 2$ or -1 .

Proof. Let $f(x) = x^5 - ax - 1$. If f is reducible, there are two possible cases: it has a linear factor or it factors as the product of an irreducible quadratic with an irreducible cubic.

In the first case it follows that f has a root $r \in \mathbb{Z}$. By the rational root theorem we know that r divides the constant term, so $r = \pm 1$. Now $f(1) = 0$ implies $a = 0$, and $f(-1) = 0$ implies $a = 2$.

For the second case, assume that

$$f(x) = (Ax^2 + bx + c)(Bx^3 + dx^2 + ex + g).$$

Since f is monic we must have $A = B = 1$ or $A = B = -1$. WLOG, we'll assume that $A = B = 1$:

$$f(x) = x^5 + (b+d)x^4 + (c+e+bd)x^3 + (g+cd+be)x^2 + (bg+ce)x + cg.$$

Therefore $d = -b$, $c + e = b^2$, $b(c - e) = g$, $bg + ce = -a$, $cg = -1$.

If $c = -1$, then $g = 1$ and thus $-b(e + 1) = 1$, implying $e = 0$ or $e = -2$. In either case, $b^2 = c + e < 0$, which is a contradiction.

If $c = 1$, then $g = -1$ and thus $b(e - 1) = 1$, implying $e = 2$ or $e = 0$. If $e = 2$ then $b^2 = 3$, which is a contradiction. So $e = 0$ and hence $b = -1$ and $a = -1$, giving the factorization:

$$f(x) = (x^2 - x + 1)(x^3 + x^2 - 1).$$

$\square$

Problem 3 [13.2.3] Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Solution. Clearly $1 + i \in \mathbb{Q}(i)$ and since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ we see that the degree of the minimal polynomial should be 2. Notice that $(i + 1)^2 - 2(i + 1) + 2 = 0$ and the polynomial $x^2 - 2x + 2$ is irreducible by the Eisenstein's criterion, therefore it is the minimal polynomial of $i + 1$.

$\square$

Problem 4 [13.2.13] Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Observe that each α_i satisfies $x^2 - \alpha_i^2 \in \mathbb{Q}[x]$, hence

$$[\mathbb{Q}(\alpha_1, \dots, \alpha_i) : \mathbb{Q}(\alpha_1, \dots, \alpha_{i-1})] = 1 \text{ or } 2.$$

Therefore, $[F : \mathbb{Q}] = 2^t$, for some natural number $t \leq n$. If $\sqrt[3]{2} \in F$, then $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subseteq F$, so

$$2^t = [F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot [F : \mathbb{Q}(\sqrt[3]{2})],$$

implying $3|2^t$, which is a contradiction. Thus, $\sqrt[3]{2} \notin F$. □

Problem 5. Let $m, n \geq 1$ be positive integers such that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is an extension of finite fields. Show that $m|n$.

Proof. We shall use the following result.

Lemma 1. *Let F/K be a finite field extension such that K has q elements. Then F has q^n elements, where $n = [F : K]$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis of F (as a vector space) over K . Then each element of F can be written as a linear combination $c_1\alpha_1 + \dots + c_n\alpha_n$, where $c_i \in K$. Since each c_i can take q possible values, it follows that F has q^n elements. □

Now, if $d = [F_{p^n} : F_{p^m}]$ then by the lemma it follows that $p^n = (p^m)^d$, showing that $m|n$. □

Homework 2

Due Wednesday, April 17, at noon

You are encouraged to work together with others, but you must write up the solutions on your own. All numbered exercises are from Dummit and Foote, third edition.

1. (5pt) 13.2.14
2. (5pt) (Restatement of 13.4.5) Let F be a field and let $P \in F[X]$ with splitting field E/F .
 - (a) Show that for any element α of some extension of F , $E(\alpha)$ is a splitting field of P over $F(\alpha)$.
 - (b) Show that every irreducible polynomial $Q \in F[X]$ with a root in E has all roots in E . [Hint: Read the hint from the book.]
3. (5pt) 13.4.6
4. (5pt) Let α and β be two algebraic elements over a field F . Assume that the degree of the minimal polynomial of α over F is relatively prime to the degree of the minimal polynomial of β over F . Prove that the minimal polynomial of β over F is irreducible over $F(\alpha)$.
5. (5pt) Let E and K be finite field extensions of F such that $[EK : F] = [E : F][K : F]$. Show that $K \cap E = F$.

HOMEWORK 2 SOLUTIONS

Problem 1 [13.2.14] Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. If $\alpha \notin F(\alpha^2)$ then $F(\alpha^2)$ is a proper subfield of $F(\alpha)$. Moreover α satisfies $x^2 - \alpha^2 \in F(\alpha^2)$, so $[F(\alpha) : F(\alpha^2)] = 2$. However,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2 \cdot [F(\alpha^2) : F],$$

which contradicts the fact that $[F(\alpha) : F]$ is odd. Thus $\alpha \in F(\alpha^2)$, and therefore $F(\alpha) = F(\alpha^2)$. $\square$

Problem 2. Let F be a field and let $f \in F[X]$ with a splitting field E over F .

- (a) Show that for any element α of some extension of F , $E(\alpha)$ is a splitting field of f over $F(\alpha)$.
- (b) Show that every irreducible polynomial $g \in F[X]$ with a root in E has all roots in E .

Proof. (a) Since E is the splitting field of f over F , it is generated over F by the roots of f . Consequently, $E(\alpha)$ is generated by the roots as an extension of $F(\alpha)$, so $E(\alpha)$ is the splitting field of f over $F(\alpha)$.

(b) Assume that β is a root of g in E , and let γ be any other root of g in an algebraic closure of E . Since β and γ are roots of the same irreducible polynomial g , it follows from Theorem 8, Sec. 13.1, that $F(\beta) \cong F(\gamma)$. Since E is a splitting field of f over F , it follows (by (a)) that $E(\beta)$ is a splitting field of f over $F(\beta)$, and $F(\gamma)$ is a splitting field of f over $F(\gamma)$. Hence, by Theorem 27, Sec. 13.4, the F -isomorphism from $F(\beta)$ onto $F(\gamma)$ can be extended to an isomorphism from $E(\beta)$ onto $E(\gamma)$. By assumption, $\beta \in E$, thus $E \cong E(\beta) \cong E(\gamma)$, showing that $\gamma \in E$. $\square$

Remark. The converse of part (b) also holds, namely: If any irreducible polynomial $g \in F[X]$ with a root in a finite extension E of F has all of its roots in E then E is a splitting field over F . Indeed, set $E = F(\alpha_1, \dots, \alpha_n)$ and let f_i be the minimal polynomial of α_i . Since each f_i has a root in E , the hypothesis implies that each f_i splits completely in $E[X]$. Hence, it is easy to see that E is the splitting field of $f = \prod_{i=1}^n f_i$ over F .

Problem 3 [13.4.6] Let K_1 and K_2 be finite extensions of F contained in the field K , and assume both are splitting fields over F .

- (a) Prove that their composite K_1K_2 is a splitting field over F .
- (b) Prove that $K_1 \cap K_2$ is a splitting field over F .

Proof. (a) Let K_1 be the splitting field of $f \in F[x]$, and K_2 the splitting field of $g \in F[x]$. Then K_1K_2 contains the roots of both f and g . Therefore K_1K_2 is the splitting field of the polynomial $h = fg$ over F .

(b) Let $g(x) \in F[x]$ be an irreducible polynomial with a root in $K_1 \cap K_2$. This means that g has a root in K_1 and also a root in K_2 . Since both K_1 and K_2 are splitting fields, we can use the previous remark to conclude that g splits completely in K_1 and in K_2 . Hence g splits completely in $K_1 \cap K_2$, showing that $K_1 \cap K_2$ is a splitting field over F . $\square$

Problem 4. Let α and β be two algebraic elements over a field F . Assume that the degree of the minimal polynomial of α over F is relatively prime to the degree of the minimal polynomial of β over F . Prove that the minimal polynomial of β over F is irreducible over $F(\alpha)$.

Proof. We know that $\deg m_{\alpha,F}(x) = [F(\alpha) : F]$ and $\deg m_{\beta,F}(x) = [F(\beta) : F]$. Also

$$\begin{aligned} [F(\alpha, \beta) : F] &= [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] \\ &= [F(\alpha, \beta) : F(\beta)][F(\beta) : F]. \end{aligned}$$

Since $\gcd(\deg m_{\alpha,F}(x), \deg m_{\beta,F}(x)) = 1$ it follows that $[F(\beta) : F]$ divides $[F(\alpha, \beta) : F(\alpha)]$. Equivalently, the degree of the minimal polynomial of β over $F(\alpha)$ is divisible by the degree of the minimal polynomial of β over F . Considering that the former polynomial divides the latter polynomial (by Proposition 9, Sec 13.2) we infer that the two polynomials are in fact equal. In other words, $m_{\beta,F}(x)$ remains irreducible over $F(\alpha)$, as desired. $\square$

Problem 5. Let E and K be finite field extensions of F such that $[EK : F] = [E : F][K : F]$. Show that $K \cap E = F$.

Solution 1. Let $L = K \cap E$, then

$$\begin{aligned} [EK : F] &= [E : F][K : F] = [E : L][L : F][K : L][L : F] \\ &= [E : L][K : L][L : F]^2 \\ &\geq [EK : L][L : F]^2 \text{ by Proposition 21, Sec 13.2} \\ &= [EK : F][L : F]. \end{aligned}$$

In conclusion $[L : F] = 1$ and hence $L = F$, as desired. $\square$

Solution 2. Let $\alpha_1, \dots, \alpha_n$ be an F -basis for E and let $\beta_1, \dots, \beta_m$ be an F -basis for K . By the proof of Proposition 21, Sec. 13.2, we conclude that the equality $[EK : F] = [E : F][K : F]$ implies that the set $\mathcal{B} = \{\alpha_i\beta_j\}$ is a basis for EK over F . Clearly we can choose the above bases such that $\alpha_1 = \beta_1 = 1 \in F$. Then $\mathcal{S} := \{1, \alpha_2, \dots, \alpha_n, \beta_2, \dots, \beta_m\} \subset \mathcal{B}$ so the elements of this set are linearly independent over F .

Now if $\gamma \in E \cap K$ then we can write $\gamma = \sum_{i=1}^n a_i \alpha_i = \sum_{j=1}^m b_j \beta_j$ for $a_i, b_j \in F$. It yields that $0 = (a_1 - b_1) \cdot 1 + \sum_{i=2}^n a_i \alpha_i - \sum_{j=2}^m b_j \beta_j$. By the above, the elements of $\mathcal{S}$ are linearly independent over F . Therefore $a_1 = b_1$ and $a_i = b_j = 0$ for $i, j \geq 2$. Consequently $\gamma = a_1 = b_1 \in F$ implying that $E \cap K \subseteq F$ and thus $E \cap K = F$. $\square$

Homework 3

Due Wednesday, April 24, at noon

You are encouraged to work together with others, but you must write up the solutions on your own. All numbered exercises are from Dummit and Foote, third edition.

1. 13.2.18
2. 13.5.7
3. 13.6.6
4. Let α be a real number such that $\alpha^4 = 5$.
 - (a) Is $\mathbb{Q}(i\alpha^2)$ normal over $\mathbb{Q}$?
 - (b) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}(i\alpha^2)$?
 - (c) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}$?
5. Let K be a field of characteristic p . If L is a finite extension of K such that $[L : K]$ is relatively prime to p , show that L is separable over K .

HOMEWORK 3

SOLUTIONS

Problem 1 [13.2.18] Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k . Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$.

- (a) Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root.
- (b) Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.
- (c) Show that $[k(x) : k(t)] = \left[k(x) : k\left(\frac{P(x)}{Q(x)}\right) \right] = \max(\deg P(x), \deg Q(x))$.

Proof. (a) Since $k[t]$ is an UFD and $k(t)$ is its fields of fractions, Gauss' Lemma tells us that the polynomial $P(X) - tQ(X)$ is irreducible over $(k(t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Now $(k[t])[X] = (k[X])[t]$, and $P(X) - tQ(X)$ is linear, and thus irreducible in $(k[X])[t]$. By the above, it is irreducible over $k(t)$. In addition, $P(x) - tQ(x) = P(x) - \frac{P(x)}{Q(x)}Q(x) = 0$, so x is a root.

(b) Let $n = \max(\deg P(x), \deg Q(x))$. Then $P(x) = a_n x^n + (\text{lower degree terms})$ and $Q(x) = b_n x^n + (\text{lower degree terms})$, and at least one of a_n and b_n is not zero. Clearly, $\deg(P(X) - tQ(X)) \leq n$. Note that the coefficient of X^n in $P(X) - tQ(X)$ is $a_n - tb_n$. Since $t \in k(x)$, but $t \notin k$ (as P and Q are relatively prime) it follows that $a_n - tb_n \neq 0$, and thus $\deg(P(X) - tQ(X)) = n$.

(c) We know from (a) that $P(X) - tQ(X)$ is irreducible over $k(t)$ and has x as a root, so $P(X) - tQ(X)$ is the minimal polynomial of x over $k(t)$. By (b)

$$[k(x) : k(t)] = \deg(P(X) - tQ(X)) = \max(\deg(P(x)), \deg(Q(x))).$$

□

Problem 2 [13.5.7] Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K . Conclude that there exist inseparable finite extensions of K .

Proof. Since $K \neq K^p$ there exists an element $c \in K$ such that $c \notin K^p$. Consider $f(x) = x^p - c \in K[x]$, and let α be a root of f in an algebraic closure of K , i.e. $c = \alpha^p$. We obtain that $f(x) = x^p - c = x^p - \alpha^p = (x - \alpha)^p$ so α is the unique root (of multiplicity p) of f , showing that f is inseparable over K .

Now suppose that $g(x) \in K[x]$ is an irreducible factor of $f(x)$. By the above, it must be of the form $g(x) = (x - \alpha)^q$ for some $q \leq p$. By the binomial expansion $g(x) = (x - \alpha)^q = x^q - qx^{q-1}\alpha + \dots + (-\alpha)^q \in K[x]$. In particular $q\alpha \in K$, and since $\alpha \notin K$ (for otherwise, $c = \alpha^p \in K^p$) we infer that $q = p$ and $g = f$. Therefore, $f(x)$ is an irreducible inseparable polynomial over K . In conclusion, $K(\alpha)$ is an inseparable finite extension of K . $\square$

Problem 3 [13.6.6] Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

Proof. Let $-\zeta_n$ be a root of $\Phi_n(-x)$, then $(-\zeta_n)^{2n} = (-1)^{2n} = 1$ and so $-\zeta_n$ is a root of $\Phi_{2n}(x)$.

Conversely, if ζ_{2n} is a root of $\Phi_{2n}(x)$ then $\zeta_{2n} = e^{2ki\pi/2n} = e^{ki\pi/n}$ for some positive integer k , which is relatively prime to $2n$. Hence $-(\zeta_{2n})^n = -e^{ki\pi} = 1$, showing that ζ_{2n} is a root of $\Phi_n(-x)$.

Consequently, the two polynomials $\Phi_{2n}(x)$ and $\Phi_n(-x)$ share the same roots. Moreover, both of them are monic, irreducible, and of the same degree (as $\phi(2n) = \phi(2)\phi(n) = \phi(n)$ for n -odd) meaning that they should in fact be equal. $\square$

Problem 4. Let α be a real number such that $\alpha^4 = 5$.

(a) Is $\mathbb{Q}(i\alpha^2)$ normal over $\mathbb{Q}$?

(b) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}(i\alpha^2)$?

(c) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}$?

Solution. (a) The roots of the polynomial $x^2 + 5 \in \mathbb{Q}[x]$ are $\pm i\alpha^2$, so this polynomial splits completely in $\mathbb{Q}(i\alpha^2)$. Therefore $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ is normal.

(b) The roots of the polynomial $x^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[x]$ are $\pm(\alpha + i\alpha)$, so this polynomial splits completely in $\mathbb{Q}(\alpha + i\alpha)$. Therefore $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}(i\alpha^2)$ is normal.

(c) Since $\alpha + i\alpha$ satisfies the polynomial $f(x) = x^4 + 20$ we get that $F = \mathbb{Q}(\alpha + i\alpha)$ is an extension of degree at most 4 over $\mathbb{Q}$. Now if $F/\mathbb{Q}$ were normal, then this extension would contain all roots of f , so in particular $\alpha - i\alpha \in F$. But then α and i are in F , so $\mathbb{Q}(\alpha, i) \subset F$. However, it is not hard to see that $\mathbb{Q}(\alpha, i)$ is of degree 8 over $\mathbb{Q}$ which contradicts the above fact that $[F : \mathbb{Q}] \leq 4$. In conclusion, F is not normal over $\mathbb{Q}$.

Remark. Notice that every degree 2 extension is normal. Indeed, if $[K : F] = 2$ then $K = F(\alpha)$, where α is a root of an irreducible (quadratic) polynomial f over F . But then $f(x) = (x - \alpha)g(x)$ with $\deg g = 1$. Therefore f splits in K , so K/F is normal. $\square$

Problem 5. Let K be a field of characteristic p . If L is a finite extension of K such that $[L : K]$ is relatively prime to p , show that L is separable over K .

Proof. Since L/K is a finite extension we can write $L = K(\alpha_1, \dots, \alpha_n)$. It is enough to show that each α_i is separable over F . Choose any α_i (call it α) and let $f(x)$ be its minimal polynomial over K . If $f(x)$ were not separable over K , then (by Proposition 33, Sec 13.5) $f(x)$ and $D_x(f(x))$ would not be relatively prime. By definition $f(x)$ is irreducible, so it must be the case that $f(x) \mid D_x(f(x))$. Since $|f(x)| > |D_x(f(x))|$ it follows that $D_x(f(x)) = 0$.

Now denote by $m = \deg(f(x))$, then clearly $m \mid [L : K]$. Since p is a prime not dividing $[L : K]$, we have that $p \nmid m$, and thus the derivative $D_x(f(x))$ is not identically 0, which is a contradiction. Therefore, $f(x)$ is separable over K . □

Homework 4

Due Wednesday, May 1st, at noon

You are encouraged to work together with others, but you must write up the solutions on your own. All numbered exercises are from Dummit and Foote, third edition.

1. 14.1.7
2. 14.1.8
3. 14.2.13
4. If α is a complex root of $x^6 + x^3 + 1$ find all field homomorphisms $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$.
5. Let $d > 0$ be a square-free integer. Show that $\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})$ is Galois and determine its Galois group explicitly. Show that $\text{Gal}(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}))$ is isomorphic to the dihedral group with 8 elements by giving an explicit isomorphism.

HOMEWORK 4

SOLUTIONS

Problem 1 [14.1.7]

- (a) Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma(a) < \sigma(b)$ for every $a, b \in \mathbb{R}$.
- (b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma(b) < \frac{1}{m}$ for every positive integer m . Conclude that σ is a continuous map on $\mathbb{R}$.
- (c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$, and let $a, b \in \mathbb{R}$ be arbitrary real numbers.

(a) Obviously, $\sigma(a^2) = (\sigma(a))^2$ so σ takes positive reals to positive reals. If $a < b$ then since $\mathbb{Q}$ is dense in $\mathbb{R}$ there exists $u \in \mathbb{Q}$ such that $a < u < b$. We obtain

$$u = \sigma(u) = \sigma(u - a + a) = \sigma(u - a) + \sigma(a) > \sigma(a),$$

and similarly $u < \sigma(b)$, yielding $\sigma(a) < u < \sigma(b)$.

(b) Suppose that $|a - b| < \frac{1}{m}$, for some $m \in \mathbb{Z}$. In view of (a), we get

$$-\frac{1}{m} = \sigma\left(-\frac{1}{m}\right) < \sigma(a - b) = \sigma(a) - \sigma(b) < \sigma\left(\frac{1}{m}\right) = \frac{1}{m}.$$

By definition σ is continuous if for any $\epsilon > 0$, $\exists \delta > 0$ such that $|\sigma(x) - \sigma(y)| < \epsilon$, whenever $|x - y| < \delta$. Now fixing $\epsilon > 0$, let $\delta = \frac{1}{m} < \epsilon$, for some $m \in \mathbb{Z}$. If $|x - y| < \delta$, then by the above

$$|\sigma(x) - \sigma(y)| < \frac{1}{m} < \epsilon,$$

showing that σ is continuous.

(c) Let $x \in \mathbb{R}$ and $\epsilon > 0$. Since σ is continuous $\exists \delta > 0$ such that $|\sigma(x) - \sigma(y)| < \frac{\epsilon}{2}$, whenever $|x - y| < \delta$. Set $\rho = \min(\frac{\epsilon}{2}, \delta)$ and let $a \in \mathbb{Q}$ such that $|x - a| < \rho$. Then

$$\begin{aligned} |\sigma(x) - x| &= |\sigma(x) - a + (a - x)| \\ &\leq |\sigma(x) - \sigma(a)| + |a - x| \\ &< \frac{\epsilon}{2} + \rho \leq \epsilon, \text{ implying that } \sigma(x) = x. \end{aligned}$$

Consequently, the only automorphism of $\mathbb{R}$ fixing $\mathbb{Q}$ is just the identity.

□

Problem 2 [14.1.8] Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the *fractional linear transformations* determined by $t \mapsto \frac{at+b}{ct+d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$.

Proof. Let $\phi : k(t) \rightarrow k(t)$ be defined by $\phi(f(t)) = f\left(\frac{at+b}{ct+d}\right)$, for $f(t) \in k(t)$.

If $f, g \in k(t)$ then

$$\phi((f+g)(t)) = (f+g)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right) + g\left(\frac{at+b}{ct+d}\right) = \phi(f(t)) + \phi(g(t)),$$

$$\phi((fg)(t)) = (fg)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right) g\left(\frac{at+b}{ct+d}\right) = \phi(f(t))\phi(g(t)),$$

so ϕ is a homomorphism.

Assume $\phi(f(t)) = \phi(g(t))$ for some $f(t), g(t) \in k(t)$. Then

$$f\left(\frac{at+b}{ct+d}\right) = g\left(\frac{at+b}{ct+d}\right) \implies f = g \text{ in } k\left(\frac{at+b}{ct+d}\right).$$

By [13.2.18] we infer that

$$\left[k(t) : k\left(\frac{at+b}{ct+d}\right)\right] = \max(\deg(at+b), \deg(ct+d)) = 1,$$

so $k(t) = k\left(\frac{at+b}{ct+d}\right)$ and thus $f = g$ in $k(t)$, showing that ϕ is injective. Moreover, the above implies that $\text{Im}(\phi) = k\left(\frac{at+b}{ct+d}\right) = k(t)$, so ϕ is surjective. In conclusion, ϕ is an automorphism. It remains to see that ϕ fixes the constant functions, which are precisely the elements of k , hence ϕ fixes k .

Conversely, let ϕ be an automorphism of $k(t)$ fixing k , and $f(t) = \frac{\sum_i^m a_i t^i}{\sum_i^n b_i t^i} \in k(t)$. Observe that

$$\phi(f(t)) = \frac{\phi(\sum_i^m a_i t^i)}{\phi(\sum_i^n b_i t^i)} = \frac{\sum_i^m a_i \phi(t^i)}{\sum_i^n b_i \phi(t^i)} = f(h(t)),$$

where $h(t) = \frac{P(t)}{Q(t)}$ and P, Q are relatively prime over k .

Now $\text{Im}(\phi) = k(h(t)) = k\left(\frac{P(t)}{Q(t)}\right)$, and since ϕ is an automorphism $\text{Im}(\phi) = k(t)$. Hence by [13.2.18],

$$\max(\deg(P(t)), \deg(Q(t))) = [k(t) : k(h(t))] = 1,$$

proving that $P(t) = at + b$ and $Q(t) = ct + d$, for some $a, b, c, d \in k$. Finally, note that if $c = 0$ then $a \neq 0$ (and clearly $d \neq 0$), for otherwise P and Q would be constants, and not relatively prime. Similarly, if $c \neq 0$ then $\frac{ad}{c} \neq b$, for otherwise $at+b = \frac{a}{c}(ct+d)$. In either case, $ad - bc \neq 0$. Therefore, the automorphisms of the rational function field $k(t)$ that fix k are precisely the fractional linear transformations. □

Problem 3 [14.2.13] Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

Proof. Let f be a cubic with a splitting field K over $\mathbb{Q}$, such that $G := \text{Gal}(K/\mathbb{Q})$ is the cyclic group of order 3. If f has only one real root, then the remaining two form a pair of conjugates. Now, complex conjugation τ fixes $\mathbb{Q}$, so $\tau \in G$. However the order of τ is 2, which does not divide $|G| = 3$, leading to a contradiction. $\square$

Problem 4. If α is a complex root of $x^6 + x^3 + 1$ find all field homomorphisms $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$.

Proof. Any field homomorphism will map the identity to 0 or to 1, so it will either be the zero homomorphism or it will fix $\mathbb{Q}$. Thus it's enough to find all homomorphisms σ fixing $\mathbb{Q}$. Now $\alpha^6 + \alpha^3 + 1 = 0$ implies that $\sigma(\alpha)^6 + \sigma(\alpha)^3 + 1 = 0$, showing that any homomorphism sends α to another root of $x^6 + x^3 + 1$. Since $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$, the roots of $x^6 + x^3 + 1$ are just $\{\omega_k = e^{2\pi i \frac{k}{9}} \mid k = 1, 2, 4, 5, 7, 8\}$. Note that each automorphism is determined by where ω_1 gets sent to. For instance, if $\sigma(\omega_1) = \omega_2$, then $\sigma(\omega_2) = \omega_4$, $\sigma(\omega_4) = \omega_8$, $\sigma(\omega_8) = \omega_5$, $\sigma(\omega_5) = \omega_1$, $\sigma(\omega_7) = \omega_3$ and $\sigma(\omega_3) = \omega_6$. Thus the possible homomorphisms are just the ones mapping ω_1 to ω_k , for $k = 1, 2, 4, 5, 7, 8$. $\square$

Problem 5. Let $d > 0$ be a square-free integer. Show that $\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})$ is Galois and determine its Galois group explicitly. Show that $\text{Gal}(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}))$ is isomorphic to the dihedral group with 8 elements by giving an explicit isomorphism.

Proof. Note that $\text{Aut}(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}))$ is determined by the action on the generators $\theta = \sqrt[8]{d}$ and i . Consider

$$r : \begin{cases} \sqrt[8]{d} \mapsto \zeta^6 \sqrt[8]{d} \\ i \mapsto i \end{cases} \quad \text{and} \quad s : \begin{cases} \sqrt[8]{d} \mapsto \sqrt[8]{d} \\ i \mapsto -i \end{cases}$$

Then it is not hard to see that any automorphism generated by r and s fixes $\mathbb{Q}(\sqrt{d})$. Moreover, $\mathbb{Q}(\sqrt[8]{d}, i)$ is an extension of degree 8 over $\mathbb{Q}(\sqrt{d})$. Note that $r^4 = s^2 = 1$ and $rsr = s$, which is a presentation of the dihedral group. Therefore

$8 = |D_8| = |\langle r, s \mid r^4 = s^2 = 1, rsr = s \rangle| \leq |\text{Aut}(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}))| \leq [\mathbb{Q}(\sqrt[8]{d}, i) : \mathbb{Q}(\sqrt{d})] = 8$, showing that $\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})$ is Galois, and $\text{Gal}(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})) = D_8$. $\square$

Homework 5

Due Wednesday, May 15, at noon

You are encouraged to work together with others, but you must write up the solutions on your own.
All numbered exercises are from Dummit and Foote, third edition.

1. 14.2.3
2. 14.2.16
3. 14.2.17
4. 14.2.18
5. 14.2.22

HOMEWORK 5

SOLUTIONS

Problem 1 [14.2.3] Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine all the subfields of the splitting field of this polynomial.

Solution. It is easy to see that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the splitting field of the polynomial $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$. Moreover $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$ is a $\mathbb{Q}$ -basis for K and thus $[K : \mathbb{Q}] = 8$. So if $G = \text{Gal}(K/\mathbb{Q})$ then $|G| = 8$.

Consider the following automorphisms (of order 2 in G)

$$\sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} \quad \sigma_3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} \quad \sigma_5 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

then obviously

$$G = \langle \sigma_2, \sigma_3, \sigma_5 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Notice that G is abelian, implying that all of its subgroups are normal. Now by the Fundamental Theorem of Galois theory, every *normal* subgroup $H \leq G$ corresponds to a subfield K^H , which is a splitting field over $\mathbb{Q}$. Since $|H|$ divides 8, we distinguish 4 cases:

- $|H| = 1$, then clearly $K^H = K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
- $|H| = 2$, then H contains the identity and an element of order 2, so it can be any of the following 7 groups: $\{1, \sigma_2\}$, $\{1, \sigma_3\}$, $\{1, \sigma_5\}$, $\{1, \sigma_2\sigma_3\}$, $\{1, \sigma_3\sigma_5\}$, $\{1, \sigma_5\sigma_2\}$, $\{1, \sigma_2\sigma_3\sigma_5\}$. By looking at the action on the basis elements we find that the corresponding fixed subfields of the above groups are $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{15})$, $\mathbb{Q}(\sqrt{3}, \sqrt{10})$, $\mathbb{Q}(\sqrt{6}, \sqrt{10})$.
- $|H| = 4$, then H contains the identity, two distinct elements of order 2, and their product so it can be any of the following 7 groups: $\{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$, $\{1, \sigma_3, \sigma_5, \sigma_3\sigma_5\}$, $\{1, \sigma_5, \sigma_2, \sigma_5\sigma_2\}$, $\{1, \sigma_2, \sigma_3\sigma_5, \sigma_2\sigma_3\sigma_5\}$, $\{1, \sigma_3, \sigma_2\sigma_5, \sigma_2\sigma_3\sigma_5\}$, $\{1, \sigma_5, \sigma_2\sigma_3, \sigma_2\sigma_3\sigma_5\}$, $\{1, \sigma_2\sigma_3, \sigma_3\sigma_5, \sigma_5\sigma_2\}$. Their corresponding fixed subfields are $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{30})$.
- $|H| = 8$, then $K^H = \mathbb{Q}$.

□

Problem 2 [14.2.16]

- (a) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.
- (b) Show that the roots of this quartic are $\alpha_1 = \sqrt{1 + \sqrt{3}}$, $\alpha_2 = \sqrt{1 - \sqrt{3}}$, $\alpha_3 = -\sqrt{1 + \sqrt{3}}$, $\alpha_4 = -\sqrt{1 - \sqrt{3}}$.
- (c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
- (d) Prove that K_1, K_2 and K_1K_2 are Galois over F with $\text{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\text{Gal}(K_1K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F .
- (e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

Proof. (a) The polynomial $x^4 - 2x^2 - 2$ is irreducible by Eisenstein's criterion for $p = 2$.

(b) Note that $(\pm\sqrt{1 \pm \sqrt{3}})^4 - 2(\pm\sqrt{1 \pm \sqrt{3}})^2 - 2 = (4 \pm 2\sqrt{3}) - 2(1 \pm \sqrt{3}) - 2 = 0$.

(c) Observe that α_1 is real, while α_2 is complex, so $K_1 \neq K_2$. Now $F \subseteq K_1 \cap K_2$. K_1, K_2 are each of degree 4, and they're not equal, so $2 \leq [K_1 \cap K_2 : \mathbb{Q}] < 4$. Therefore $K_1 \cap K_2 = F$.

(d) We have the following factorization

$$x^4 - 2x^2 - 2 = (x^2 - 1 - \sqrt{3})(x^2 - 1 + \sqrt{3}) \in F[x],$$

and clearly K_1 is the splitting field of $x^2 - 1 - \sqrt{3} \in F[x]$ so K_1/F is Galois. Similarly, K_2/F is also Galois.

Now K_1K_2 is the splitting field of the polynomial $x^4 - 2x^2 - 2$ over F and $\text{Gal}(K_1K_2/F)$ is generated by

$$\tau : \begin{cases} \alpha_1 \mapsto \alpha_1 \\ \alpha_2 \mapsto \alpha_4 \end{cases} \quad \sigma : \begin{cases} \alpha_1 \mapsto \alpha_3 \\ \alpha_2 \mapsto \alpha_2 \end{cases}$$

so it has the structure of the Klein 4-group. The subgroup $\{1, \tau\}$ corresponds to the fixed field K_1 , $\{1, \sigma\}$ corresponds to K_2 , $\{1, \sigma\tau\}$ corresponds to $F(\sqrt{-2})$, the identity subgroup corresponds to K_1K_2 , and $\{1, \sigma, \tau, \sigma\tau\}$ corresponds to F .

(e) Since K_1K_2 is the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ we obtain $[K_1K_2 : \mathbb{Q}] = [K_1K_2 : F][F : \mathbb{Q}] = 4 \cdot 2 = 8$ so $G = \text{Gal}(K_1K_2/\mathbb{Q})$ is of order 8. From the previous part, we see that G has at least 3 subgroups of order 2. Also, G is not abelian. Since the only nonabelian subgroups of order 8 are D_8 and Q_8 , we conclude that G must be the dihedral group. □

Problem 3 [14.2.17] Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leq \text{Gal}(L/F)$ be the subgroup corresponding to K . Define the norm of α from K to F to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where the product is taken over all F -embeddings of K into an algebraic closure of F (so over a set of coset representatives for H in $\text{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory). This is a product of conjugates of α .

- (a) Prove that $N_{K/F}(\alpha) \in F$.
- (b) Prove that the norm is a multiplicative map.
- (c) Let $K = F(\sqrt{D})$, prove that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.
- (d) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F . Let $n = [K : F]$. Prove that $d|n$, that there are d distinct Galois conjugates of α which are all repeated n/d times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Proof. (a) First we need to check that the product in the definition of the norm is well defined. Indeed, since K is the fixed field of H , the elements of a coset $\sigma H \subset \text{Gal}(L/F)$ all correspond to the same embedding σ . So if I and J are two sets of coset representatives for H , then

$$\prod_{\sigma \in I} \sigma(\alpha) = \prod_{\sigma \in J} \sigma(\alpha),$$

showing that $N_{K/F}(\alpha)$ is well defined.

Now if I is a set of coset representatives for H , then for any $\tau \in \text{Gal}(L/F)$, τI is also a complete set of representatives, say S . This implies that

$$\tau N_{K/F}(\alpha) = \tau \prod_{\sigma \in I} \sigma(\alpha) = \prod_{\sigma \in I} \tau \sigma(\alpha) = \prod_{\sigma \in S} \sigma(\alpha) = N_{K/F}(\alpha).$$

In other words $N_{K/F}(\alpha)$ is fixed by $\text{Gal}(L/F)$, so it lies in F .

(b) Note that

$$N_{K/F}(\alpha\beta) = \prod_{\sigma} \sigma(\alpha\beta) = \prod_{\sigma} \sigma(\alpha) \prod_{\sigma} \sigma(\beta) = N_{K/F}(\alpha) N_{K/F}(\beta).$$

(c) If $K = F(\sqrt{D})$ is a quadratic extension of F , then K/F is necessarily Galois. In this case, the only non-identity element of $\text{Gal}(K/F)$ is the map $\sqrt{D} \mapsto -\sqrt{D}$. Hence

$$N_{K/F}(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

(d) Because $F \subseteq F(\alpha) \subseteq K$, it is clear that $d = [F(\alpha) : F]$ divides $n = [K : F]$.

Now $F \subseteq K \subseteq L$ and L is separable over F (being Galois), thus K is also separable over F . Recall that the roots of the minimal polynomial must be precisely the Galois conjugates of α , and in view of the above m_α doesn't have multiple roots. Since $\deg(m_\alpha) = d$, there are exactly d of them.

Furthermore, there are n embeddings of K into an algebraic closure of F . Each of these embeddings sends α to a Galois conjugate (of which there are d), hence each conjugate appears n/d times in the product defining the norm. So if $\{\alpha_1, \dots, \alpha_d\}$ are the roots of m_α , then

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \left(\prod_{i=1}^d \alpha_i \right)^{n/d}.$$

Considering that $a_0 = (-1)^d \prod_{i=1}^d \alpha_i$ we obtain

$$N_{K/F}(\alpha) = (-1)^n a_0^{n/d}.$$

□

Problem 4 [14.2.18] With the notation as in the previous problem, define the trace of α from K to F to be

$$\text{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha),$$

a sum of Galois conjugates of α .

(a) Prove that $\text{Tr}_{K/F}(\alpha) \in F$.

(b) Prove that the trace is an additive map.

(c) Let $K = F(\sqrt{D})$, prove that $\text{Tr}_{K/F}(a + b\sqrt{D}) = 2a$.

(d) Let $m_{\alpha}(x)$ as in the previous problem. Prove that $\text{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$.

Proof. (a) This follows by the same reasoning as in the problem above.

(b) Notice that

$$\text{Tr}_{K/F}(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha) + \sum_{\sigma} \sigma(\beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta).$$

(c) In view of the previous problem

$$\text{Tr}_{K/F}(a + b\sqrt{D}) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a.$$

(d) As we saw in the previous problem, each of the d distinct Galois conjugates of K is repeated n/d times in the sum defining the trace. Hence

$$\text{Tr}_{K/F}(\alpha) = \frac{n}{d} \left(\sum_{i=1}^d \alpha_i \right).$$

Since $\sum_{i=1}^d \alpha_i = -a_{d-1}$, it follows that $\text{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$. □

Problem 5 [14.2.22] Suppose that K/F is a Galois extension and let σ be an element of the Galois group.

(a) Suppose $\alpha \in K$ is of the form $\alpha = \frac{\beta}{\sigma\beta}$ for some nonzero $\beta \in K$. Prove that $N_{K/F}(\alpha) = 1$.

(b) Suppose $\alpha \in K$ is of the form $\alpha = \beta - \sigma\beta$ for some $\beta \in K$. Prove that $\text{Tr}_{K/F}(\alpha) = 0$.

Proof. a) By the definition of the norm we have that for $\beta \in K$ and $\sigma \in G = \text{Gal}(K/F)$:

$$N_{K/F}(\sigma\beta) = \prod_{\tau \in G} \tau(\sigma\beta) = \prod_{\rho \in G} \rho\beta = N_{K/F}(\beta).$$

Thus if $\alpha = \frac{\beta}{\sigma\beta}$ then $N_{K/F}(\alpha) = \frac{N_{K/F}(\beta)}{N_{K/F}(\sigma\beta)} = 1$.

b) Similarly, one has that $\text{Tr}_{K/F}(\beta) = \text{Tr}_{K/F}(\sigma\beta)$. Hence, if $\alpha = \beta - \sigma\beta$ then $\text{Tr}_{K/F}(\alpha) = \text{Tr}_{K/F}(\beta) - \text{Tr}_{K/F}(\sigma\beta) = 0$. □

Homework 6

Due Wednesday, May 22, at noon

You are encouraged to work together with others, but you must write up the solutions on your own.
All numbered exercises are from Dummit and Foote, third edition.

1. 14.2.23
2. 14.2.29
3. 14.2.31
4. 14.3.7
5. 14.3.8

HOMEWORK 6

SOLUTIONS

Problem 1 [14.2.23] Let K be a Galois extension of F with cyclic Galois group of order n generated by σ . Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that $\alpha = \frac{\beta}{\sigma\beta}$ for some nonzero $\beta \in K$.

Proof. By the linear independence of the characters $1, \sigma, \dots, \sigma^{n-1}$ (Th 7, Sec 14.2), $\exists \theta \in K$ such that

$$\beta := \theta + \alpha \sigma(\theta) + (\alpha \sigma \alpha) \sigma^2(\theta) + \dots + (\alpha \sigma \alpha \dots \sigma^{n-2} \alpha) \sigma^{n-1}(\theta) \neq 0.$$

Considering that $\sigma^n(\theta) = \theta$ and $N(\alpha) = \alpha \sigma \alpha \dots \sigma^{n-1} \alpha = 1$ we obtain

$$\begin{aligned} \sigma(\beta) &= \sigma(\theta) + \sigma(\alpha) \sigma^2(\theta) + \dots + (\sigma(\alpha) \dots \sigma^{n-1}(\alpha)) \sigma^n(\theta) \\ &= \sigma(\theta) + \sigma(\alpha) \sigma^2(\theta) + \dots + \frac{1}{\alpha} \cdot \theta \\ &= \frac{\alpha \sigma(\theta) + \alpha \sigma(\alpha) \sigma^2(\theta) + \dots + \theta}{\alpha} \\ &= \frac{\beta}{\alpha}, \text{ showing that } \alpha = \frac{\beta}{\sigma\beta}. \end{aligned}$$

□

Problem 2 [14.2.29] Let k be a field and let $k(t)$ be the field of rational functions in the variable t . Define the maps σ and τ of $k(t)$ to itself by $\sigma f(t) = f(\frac{1}{1-t})$ and $\tau f(t) = f(\frac{1}{t})$ for $f(t) \in k(t)$.

(a) Prove that σ and τ are automorphisms of $k(t)$ and that $G := \langle \sigma, \tau \rangle \cong S_3$.

(b) Prove that the element $s = \frac{(t^2-t+1)^3}{t^2(t-1)^2}$ is fixed by all the elements of G .

(c) Prove that $k(s)$ is precisely the fixed field of G in $k(t)$.

Proof. (a) From HW 4 ([14.1.8]) we know that the automorphisms of $k(t)$ are given by the fractional linear transformation $t \mapsto \frac{at+b}{ct+d}$, with $ad-bc \neq 0$. Clearly, the maps $\sigma : t \mapsto \frac{1}{1-t}$ and $\tau : t \mapsto \frac{1}{t}$ satisfy this requirement, so σ and τ are automorphisms of $k(t)$.

Moreover, it's easy to check that $\sigma^3 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$, which is a presentation for the dihedral group of order 6. Thus $G = \langle \sigma, \tau \rangle \cong D_6 \cong S_3$.

(b) It's enough to verify that s is fixed by the two generators of G . Indeed

$$\sigma(s) = \frac{\left(\left(\frac{1}{1-t}\right)^2 - \frac{1}{1-t} + 1\right)^3}{\left(\frac{1}{1-t}\right)^2 \left(\frac{1}{1-t} - 1\right)^2} = \frac{(t^2 - t + 1)^3}{t^2(t-1)^2} = s \text{ and } \tau(s) = \frac{\left(\frac{1}{t^2} - \frac{1}{t} + 1\right)^3}{\frac{1}{t^2} \left(\frac{1}{t} - 1\right)^2} = \frac{(t^2 - t + 1)^3}{t^2(t-1)^2} = s.$$

(c) If $(k(t))^G$ is the fixed field of G in $k(t)$, then in view of (b): $k(s) \subseteq (k(t))^G \subseteq k(t)$. Now by (a) we find that $[k(t) : (k(t))^G] = |G| = |S_3| = 6$. Moreover, by HW 3 ([13.2.18]) we infer that $[k(t) : k(s)] = \max(\deg(t^2 - t + 1)^3, \deg t^2(t-1)^2) = 6$. By the multiplicativity of degrees $[k(t) : k(s)] = [k(t) : (k(t))^G][(k(t))^G : k(s)]$, which implies that $[(k(t))^G : k(s)] = 1$ and hence $(k(t))^G = k(s)$. $\square$

Problem 3 [14.2.31] Let K be a finite extension of F of degree n . Let α be an element of K .

- Prove that α acting by left multiplication on K is an F -linear transformation T_α of K .
- Prove that the minimal polynomial for α over F is the same as the minimal polynomial for the linear transformation T_α .
- Prove that the trace $\text{Tr}_{K/F}(\alpha)$ is the trace of the $n \times n$ matrix defined by T_α . Prove that the norm is the determinant of T_α .

Proof. (a) Let $T_\alpha : K \rightarrow K$ be defined as $T_\alpha(x) = \alpha x$, for all $x \in K$. Pick any $x, y \in K$ and $a \in F$, then $T_\alpha(ax + y) = \alpha(ax + y) = a\alpha x + \alpha y = aT_\alpha(x) + T_\alpha(y)$, showing that T_α is F -linear.

(b) Let $m(x) = x^d + \dots + a_1x + a_0$ be the minimal polynomial of α over F , and let $f(x)$ be the minimal polynomial of T_α . Since $m(\alpha) = 0$ and $T_\alpha^m(x) = \alpha^m x$ (for all integers m) we get that

$$(m(T_\alpha))(x) = (T_\alpha^d + \dots + a_1T_\alpha + a_0)(x) = (\alpha^d + \dots + a_1\alpha + a_0)x = 0.$$

Hence $m(T_\alpha) = 0$, which implies that $f(x) | m(x)$. Since $m(x)$ is irreducible, we should necessarily have $m(x) = f(x)$.

(c) Let $p(x) = x^n + \dots + b_1x + b_0$ be the characteristic polynomial of T_α . From Ma 1b (or Prop 20, Sec. 12.2), we know that $p(x)$ and $m(x)$ have the same roots (not counting multiplicities) and $m(x) | p(x)$. As $m(x)$ is irreducible, all irreducible factors of $p(x)$ should be equal to $m(x)$ and thus $p(x)$ is a power of $m(x)$, i.e. $d | n$ and $p(x) = (m(x))^{n/d}$. Then by [14.2.17] and [14.2.18] we obtain that $\text{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1} = -b_{n-1} = \text{Tr}(T_\alpha)$ and $N_{K/F}(\alpha) = (-1)^n a_0^{n/d} = (-1)^n b_0 = \det(T_\alpha)$. $\square$

Problem 4 [14.3.7] Prove that one of 2, 3 or 6 is a square in $\mathbb{F}_p$ for every prime p . Conclude that the polynomial

$$f(x) = x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

has a root modulo p for every prime p but has no root in $\mathbb{Z}$.

Proof. Let y be a generator of the cyclic group $\mathbb{F}_p^\times$. Then $n \in \mathbb{F}_p^\times$ is a square iff it is an even power of y . Consequently, if 2 and 3 are not squares in $\mathbb{F}_p$, it follows that $2 \equiv y^{2k+1} \pmod{p}$ and $3 \equiv y^{2l+1} \pmod{p}$, for some $k, l \in \mathbb{Z}$. Hence $6 \equiv y^{2(k+l+1)} \pmod{p}$ is a square in $\mathbb{F}_p$.

Now $f(x)$ clearly doesn't have any integer roots. However, by the above analysis we know that there exists $\gamma \in \{2, 3, 6\}$ such that $\gamma = \alpha^2$, for some $\alpha \in \mathbb{F}_p$. Then $x - \alpha \mid x^2 - \gamma \mid f(x)$ so α is a root of f in $\mathbb{F}_p$. $\square$

Remark. Alternatively, a group-theoretic approach is also possible: Consider the group homomorphism $\phi : \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$, given by $x \mapsto x^2$. If $H := \text{Im}(\phi)$ then $H \cong \mathbb{F}_p^\times / \ker(\phi)$, and since $\ker(\phi) = \{\pm 1\}$ it follows that H has index $[\mathbb{F}_p^\times : H] = 2$ in $\mathbb{F}_p^\times$. This means that H has precisely 2 cosets in $\mathbb{F}_p^\times$. If 2 and 3 are not squares in $\mathbb{F}_p$ then $2, 3 \notin H$, so they belong to the same coset, i.e.

$2H = 3H$. Therefore $H = (2H)(2H) = (2H)(3H) = 6H$, which shows that $6 \in H$ and thus 6 is a square in $\mathbb{F}_p^\times$. This proves that one of 2, 3 or 6 is a square in $\mathbb{F}_p$.

Problem 5 [14.3.8] Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0$, $a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic.

Proof. Let α be a root of f , then $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p - \alpha - a = 0$ showing that $\alpha + 1$ is also a root. Hence the p roots of f are just $\mathcal{R} := \{\alpha + k \mid 1 \leq k \leq p\}$ (in particular f is separable). Moreover $\alpha \notin \mathbb{F}_p$, for otherwise $\alpha^p = \alpha$ and so $a = \alpha^p - \alpha = 0$, which is a contradiction. Therefore $\mathbb{F}_p(\alpha)$ is the splitting field of the separable polynomial f over $\mathbb{F}_p$, hence $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a Galois extension.

Consider the endomorphism $\sigma : \mathbb{F}_p(\alpha) \rightarrow \mathbb{F}_p(\alpha)$, which sends $\alpha \mapsto \alpha + 1$ and fixes $\mathbb{F}_p$. Note that σ has a two-sided inverse defined by a map that sends $\alpha \mapsto \alpha - 1$ and fixes $\mathbb{F}_p$. This shows that $\sigma \in \text{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$.

Any other element $\tau \in \text{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ must fix $\mathbb{F}_p$ and it must send α to a root of f , so τ is of the form $\tau : \alpha \mapsto \alpha + k$ for some $k \in \mathbb{F}_p$ (recall that $\mathcal{R}$ is the set of all the roots of f). We obtain that $\sigma^k(\alpha) = \alpha + k = \tau(\alpha)$, while σ^k and τ fix $\mathbb{F}_p$, hence $\sigma^k = \tau$. Therefore, every element of $\text{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ is a power of σ , and since $\sigma^p = 1$ we conclude that the Galois group is cyclic, of order p , generated by σ . □

Remark. The minimal polynomial $m_{\alpha, \mathbb{F}_p}$ of α over $\mathbb{F}_p$ divides $x^p - x - \alpha$ (since α is a root of f), implying that

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg m_{\alpha, \mathbb{F}_p} \leq \deg f = p.$$

Here are two ways you can notice that f is irreducible over $\mathbb{F}_p$ (and hence the equality holds above):

(i) Suppose

$$f(x) = \prod_{i=1}^p (x - (\alpha + i)) = g(x)h(x) \text{ in } \mathbb{F}_p[x].$$

Then the roots of g form a subset of $\mathcal{R}$. If $d := \deg(g) \geq 1$ then the coefficient a_{d-1} of x^{d-1} in $g(x)$ is the sum of d elements of the form $-(\alpha + k)$, so it is equal to $-d\alpha + N$ for some integer N . However $a_{d-1} \in \mathbb{F}_p$ implies that $d\alpha \in \mathbb{F}_p$, which contradicts the fact that $\alpha \notin \mathbb{F}_p$. Consequently, $f(x)$ is irreducible over $\mathbb{F}_p$ and thus it's the minimal polynomial of α over $\mathbb{F}_p$.

(ii) Let $p_1(x), \dots, p_t(x)$ be the irreducible factors of f . By adjoining any root of f to $\mathbb{F}_p$ we obtain a splitting field of f , thus each quotient $\mathbb{F}_p[x]/(p_i(x))$ is a splitting field of f , implying that all these fields are isomorphic. In particular, this means that $\deg p_1 = \dots = \deg p_t = d$. But then $d \cdot t = p$, which is possible only when $d = p$ and $t = 1$ (note that $d = 1$ and $t = p$ is impossible because f doesn't have linear factors). So f has only one irreducible factor, i.e. it's irreducible.

Homework 7

Due Wednesday, May 29, at noon

You are encouraged to work together with others, but you must write up the solutions on your own. All numbered exercises are from Dummit and Foote, third edition.

1. 14.6.35
2. 14.6.43
3. 14.6.50 a-c.
4. Determine the Galois groups of the following polynomials in $\mathbb{Q}[X]$: $X^4 - 25$, $X^4 + 4$, $X^4 + 2X^2 + X + 3$, $X^5 + X - 1$, $X^5 + 20X + 16$. [Hint: A_5 is generated by a cycle of length 3 and a cycle of length 5.]
5. Let p be a prime number. A finite extension of fields K/F is said to be a p -extension if $[K : F]$ is a power of p .
 - (a) Suppose K/F is a Galois p -extension and L/K is another Galois p -extension. Let E/L be any extension such that E/F is Galois. Show that there exists a Galois p -subextension E_p/L of E/L which is maximal among the Galois p -subextensions of E/L .
 - (b) Keep the notation from part a. Show that E_p/F is Galois and deduce that the Galois closure of L/F is a p -extension of F .
 - (c) Give an example of a (necessarily non-Galois) p -extension K/F and a Galois p -extension L/K such that the Galois closure of L/F is not a p -extension of F .

HOMEWORK 7 SOLUTIONS

Problem 1 [14.6.35] Prove that the discriminant D of the polynomial $x^n + px + q$ is given by

$$(-1)^{n(n-1)/2} n^n q^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} p^n.$$

Proof. Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x) = x^n + px + q$. Recall the following identity (obtained by taking the derivative of $\log f(x) = \sum_{i=1}^n \log(x - \alpha_i)$)

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^n \frac{1}{x - \alpha_i} \implies f'(\alpha_j) = \prod_{\substack{i=1 \\ i \neq j}}^n (\alpha_j - \alpha_i).$$

This implies that

$$D = \prod_{i < j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^n f'(\alpha_k).$$

Note that

$$f'(\alpha_i) = n\alpha_i^{n-1} + p = n\left(\frac{-p\alpha_i - q}{\alpha_i}\right) + p = -(n-1)p - \frac{nq}{\alpha_i}.$$

Hence

$$\begin{aligned} D &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \left(-(n-1)p - \frac{nq}{\alpha_i} \right) \\ &= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{\prod \alpha_i} \prod_{i=1}^n \left(-\frac{nq}{(n-1)p} - \alpha_i \right) \\ &= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{(-1)^n q} f\left(-\frac{nq}{(n-1)p}\right) \\ &= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{(-1)^n q} \left(\left(-\frac{nq}{(n-1)p}\right)^n + p\left(-\frac{nq}{(n-1)p}\right) + q \right) \\ &= (-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n. \end{aligned}$$

□

Problem 2 [14.6.43] Express each of the following in terms of the elementary symmetric functions:

(a) $A := \sum_{i \neq j} x_i^2 x_j.$

(b) $B := \sum_{i,j,k \text{ distinct}} x_i^2 x_j x_k.$

(c) $C := \sum_{i,j,k \text{ distinct}} x_i^2 x_j^2 x_k^2.$

Solution. (a) Note that

$$\begin{aligned} s_1 s_2 &= \left(\sum_{i=1}^n x_i \right) \left(\sum_{j < k} x_j x_k \right) = \sum_{j < k} \sum_{i=1}^n x_i x_j x_k \\ &= \sum_{j < k} (x_j^2 x_k + x_j x_k^2 + \sum_{i \neq j, k} x_i x_j x_k) \\ &= \sum_{j \neq k} x_j^2 x_k + 3 \sum_{i < j < k} x_i x_j x_k = A + 3s_3. \end{aligned}$$

Hence $A = s_1 s_2 - 3s_3.$

(b) Similarly,

$$\begin{aligned} s_1 s_3 &= \left(\sum_{t=1}^n x_t \right) \left(\sum_{i < j < k} x_i x_j x_k \right) = \sum_{i < j < k} \sum_{t=1}^n x_t x_i x_j x_k \\ &= \sum_{i < j < k} \left((x_i^2 x_j x_k + x_i x_j^2 x_k + x_i x_j x_k^2) + \sum_{t \neq i, j, k} x_t x_i x_j x_k \right) \\ &= \frac{B}{2} + 4s_4. \end{aligned}$$

Thus $B = 2s_1 s_3 - 8s_4.$

(c) We have,

$$\begin{aligned} s_3^2 &= \left(\sum_{i < j < k} x_i x_j x_k \right)^2 \\ &= \sum_{i < j < k} x_i^2 x_j^2 x_k^2 + \frac{1}{2} \sum_{\substack{i, j, k, l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{4} \sum_{\substack{i, j, k, l, m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + \frac{1}{36} \sum_{\substack{i, j, k, l, m, n \\ \text{distinct}}} x_i x_j x_k x_l x_m x_n \\ &= \frac{C}{6} + \frac{1}{2} \sum_{\substack{i, j, k, l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{4} \sum_{\substack{i, j, k, l, m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 20s_6. \end{aligned}$$

In addition,

$$\begin{aligned}
 s_1 s_5 &= \left(\sum_{i=1}^n x_i \right) \left(\sum_{j < k < l < m < n} x_j x_k x_l x_m x_n \right) = \sum_{j < k < l < m < n} \sum_{i=1}^n x_i x_j x_k x_l x_m x_n \\
 &= \frac{1}{4!} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 6 \sum_{i < j < k < l < m < n} x_i x_j x_k x_l x_m x_n \\
 &= \frac{1}{24} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 6s_6
 \end{aligned}$$

and thus

$$\begin{aligned}
 s_2 s_4 &= \left(\sum_{i < j} x_i x_j \right) \left(\sum_{k < l < m < n} x_k x_l x_m x_n \right) \\
 &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{6} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 15 \sum_{i < j < k < l < m < n} x_i x_j x_k x_l x_m x_n \\
 &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + 4(s_1 s_5 - 6s_6) + 15s_6 \\
 &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + 4s_1 s_5 - 9s_6.
 \end{aligned}$$

Consequently,

$$\begin{aligned}
 s_3^2 &= \frac{C}{6} + (2s_2 s_4 - 8s_1 s_5 + 18s_6) + (6s_1 s_5 - 36s_6) + 20s_6 \\
 &= \frac{C}{6} + 2s_2 s_4 - 2s_1 s_5 + 2s_6
 \end{aligned}$$

showing that $C = 6(s_3^2 - 2s_2 s_4 + 2s_1 s_5 - 2s_6)$.

□

Problem 3 [14.6.50] Suppose K is a field and $f(x) = x^3 + ax^2 + bx + c \in K[x]$ is irreducible, so the Galois group of $f(x)$ over K is either S_3 or A_3 .

- Show that the Galois group of $f(x)$ is A_3 if and only if the resultant quadratic polynomial $g(x) = x^2 + (ab - 3c)x + (b^3 + a^3c - 6abc + 9c^2)$ has a root in K .
- If $ch(k) \neq 2$ show that the Galois group is A_3 iff the discriminant of $f(x)$ is a square in K .
- If $ch(k) = 2$ show that the discriminant of $f(x)$ is always a square. Show that $f(x)$ can be taken to be of the form $x^3 + px + q$ and that the Galois group of $f(x)$ is A_3 iff the quadratic $x^2 + qx + (p^3 + q^2)$ has a root in K .

Proof. (a) Let G be the Galois group of f over K .

($\implies$) Assume that $G = A_3$. Then G is composed of the following elements

$$\sigma_1 : \begin{cases} \alpha \mapsto \alpha \\ \beta \mapsto \beta \\ \gamma \mapsto \gamma \end{cases} \quad \sigma_2 : \begin{cases} \alpha \mapsto \beta \\ \beta \mapsto \gamma \\ \gamma \mapsto \alpha \end{cases} \quad \sigma_3 : \begin{cases} \alpha \mapsto \gamma \\ \beta \mapsto \alpha \\ \gamma \mapsto \beta \end{cases}.$$

Let $\theta_1 = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ and $\theta_2 = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$. Since $\alpha + \beta + \gamma = -a$, $\alpha\beta + \beta\gamma + \gamma\alpha = b$ and $\alpha\beta\gamma = -c$, some straightforward computations show that $\theta_1 + \theta_2 = 3c - ab$ and $\theta_1\theta_2 = b^3 + a^3c - 6abc + 9c^2$, so θ_1 and θ_2 are the roots of g .

Now it is easy to check that σ_i ($1 \leq i \leq 3$) fixes θ_j ($1 \leq j \leq 2$). In particular, this implies that g has a root in K .

($\Leftarrow$) Conversely, assume that g has a root in K , say $\theta_1 \in K$. If $G = S_3$ then G contains the element

$$\sigma : \begin{cases} \alpha \mapsto \beta \\ \beta \mapsto \alpha \\ \gamma \mapsto \gamma. \end{cases}$$

This means that $\sigma(\theta_1) = \theta_2$, and since σ fixes K we must have $\theta_1 = \theta_2$. However, $\theta_2 - \theta_1 = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) \neq 0$, since α, β, γ are all distinct (f is irreducible). This is a contradiction, so $G = A_3$.

Finally, in view of the usual discriminant formula for a quadratic and (14.18') we see that

$$D(g) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc = D(f).$$

(b) Let Δ be the discriminant of g . By (a) we infer that $G = A_3$ iff $\frac{1}{2}[(3c - ab) \pm \sqrt{\Delta}] \in K$, which is equivalent to saying that Δ is a square in K . Since Δ is also the discriminant of f , the conclusion follows.

(c) If $\text{char}(K) = 2$ then $D = (ab - c)^2$ is always a square in K . As shown on page 611, f can be written in the form $x^3 + px + q$, where $p = b - \frac{a^2}{3}$ and $q = \frac{1}{27}(2a^3 - 9ab + 27c)$. In characteristic 2, it is not hard to see that the resultant polynomial becomes $g(x) = x^2 + qx + (p^3 + q^2)$ and by (a) we are done. □

Problem 4. Determine the Galois groups of the following polynomials in $\mathbb{Q}[x]$: $x^4 - 25$, $x^4 + 4$, $x^4 + 2x^2 + x + 3$, $x^5 + x - 1$, $x^5 + 20x + 16$.

Solution.

- Let $f(x) = x^4 - 25$. Then $F = \mathbb{Q}(\sqrt{5}, i)$ is a splitting field of the separable polynomial f and $[F : \mathbb{Q}] = 4$. Thus, $\text{Gal}(F/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that $\text{Gal}(F/\mathbb{Q})$ contains the following distinct elements of order two:

$$\phi : \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ i \mapsto -i \end{cases} \quad \text{and} \quad \psi : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i \mapsto i. \end{cases}$$

Therefore, $\text{Gal}(F/\mathbb{Q})$ is the Klein four-group.

- Let $f(x) = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$. The roots of f are $\pm 1 \pm i$, so the splitting field is $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$. Therefore, the Galois group of f is cyclic of order 2.
- Let $f(x) = x^4 + 2x^2 + x + 3$. Note that f is irreducible over $\mathbb{Q}$ and the discriminant $D = 3877$ is not a square. From the discussion on page 615 we infer that the Galois group of f is S_4 .
- Let $f(x) = x^5 + x - 1 = (x^2 - x + 1)(x^3 + x^2 - 1) = f_1 f_2$. Clearly, the splitting field of f_1 is $K_1 = \mathbb{Q}(\sqrt{-3})$ and $\text{Gal}(K_1/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Now, since the discriminant of f_2 is -23 the remarks on page 613 imply that the splitting field of f_2 is $K_2 = \mathbb{Q}(\theta, \sqrt{-23})$ and $\text{Gal}(K_2/\mathbb{Q}) = S_3$ (for any one of the roots θ of f_2). By [13.4.6] we know that $K_1 K_2$ is the splitting field of f . It is easy to see that $K_1 \cap K_2 = \mathbb{Q}$ so by Proposition 21 we conclude that $\text{Gal}(K_1 K_2/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times S_3$.
- Let $f(x) = x^5 + 20x + 16$. Note that f has discriminant $2^{16}5^6$ (by Problem 1), which implies that its Galois group is a subgroup of A_5 (by Prop 34, Sec. 14.6). It is straightforward to check that f is irreducible modulo 3, so it is also irreducible over $\mathbb{Q}$ and thus the Galois group contains a 5-cycle. Modulo 7, $f(x)$ factors as

$$x^5 + 20x + 16 \equiv (x - 4)(x - 5)(x^3 + 2x^2 + 5x + 5) \pmod{7},$$

showing that the Galois group also contains a 3-cycle. Since a 3-cycle and a 5-cycle generate all of A_5 , it follows that the Galois group of $f(x)$ is A_5 .

□

Problem 5. Let p be a prime. A finite extension of fields K/F is said to be a p -extension if $[K : F]$ is a power of p .

- Suppose K/F is a Galois p -extension and L/K is another Galois p -extension. Let E/L be any extension such that E/F is Galois. Show that there exists a Galois p -subextension E_p/K of E/K which is maximal among the Galois p -subextensions of E/K .
- Show that E_p/F is Galois and deduce that the Galois closure of L/F is a p -extension of F .
- Give an example of a p -extension K/F and a Galois p -extension L/K such that the Galois closure of L/F is not a p -extension of F .

Proof. (a) Since E/F is a Galois extension it follows that E/K is Galois (so finite) and thus there are only finitely many subfields of E that contain K . Let $\mathcal{S}$ be the set of all Galois p -subextensions E/K (clearly $\mathcal{S} \neq \emptyset$ because $L \in \mathcal{S}$). By the above $\mathcal{S}$ is finite, so we can write $\mathcal{S} = \{E_1, \dots, E_n\}$. Take E_p to be the the composite $E_p := E_1 E_2 \dots E_n$.

By Prop.21 (Sec.14.4) E_p is Galois over K . Moreover, since $[E_i : K] = p^{a_i}$ for some $a_i \in \mathbb{N}$, we obtain that $[E_p : K] \mid p^{\sum_{i=1}^n a_i}$ (by Cor. 20, Sec. 14.4) and therefore E_p/K is a Galois p -subextension of E/K . By construction, any Galois p -subextension of E/K is a subextension of E_p/K , thus E_p/K is maximal among the Galois p -subextensions of E/K .

(b) Let $\sigma \in \text{Gal}(E/F)$, it is enough to show that σ fixes E_p . Indeed, since K/F is Galois we have that $\sigma(K) = K$ and hence $\sigma(E_p)$ contains K . Moreover E_p and $\sigma(E_p)$ are naturally isomorphic, implying that $\sigma(E_p)/K$ is a Galois p -extension. Consider the composite $M = \sigma(E_p)E_p$, then (as

above) $[M : K] \mid [E_p : K][\sigma(E_p) : K]$ so M/K is a Galois p -extension. By maximality, we infer that $M = E_p$ and thus $\sigma(E_p) = E_p$.

Finally, note that $L \in \mathcal{S}$ so the Galois closure of L/F is a subextension of E_p/F , and hence a p -extension of F (by degree considerations).

(c) Take $F = \mathbb{Q}$, $K = L = \mathbb{Q}(\sqrt[3]{2})$. Then K/F is a 3-extension and L/K is trivially a Galois 3-extension. However, the Galois closure $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ of L is of degree 6 over F , which is not a power of 3.

□